

# IOSおよびIOS XEルータでピアツーピア通信を有効にするためのNATについて

## 内容

[概要](#)

[背景説明](#)

[NATトラバーサルの必要性](#)

[NAT用のセッショントラバーサルユーティリティ](#)

[NAT実装のタイプ](#)

[NATトラバーサルおよび対称NATに関する問題](#)

[問題の解決策](#)

[要約](#)

## 概要

このドキュメントでは、NAT(STUN)サーバ用のセッショントラバーサルユーティリティの必要性、STUNサーバに関するネットワークアドレス変換(NAT)セットアップのタイプ、NATがこのセットアップで問題を引き起こす仕組み、およびソリューションについて説明します。

## 背景説明

NATデバイスの主な目的は、ローカルエリアネットワーク(LAN)内のプライベートIPアドレスを持つデバイスが、インターネットなどのパブリックアドレス空間内のデバイスと通信できるようにすることです。ただし、NATデバイスは内部ホストがパブリックスペースに接続できるようにすることが想定されていますが、VoIP、ゲーム、WebRTC、ファイル共有などのポイントツーポイント(P2P)アプリケーションでは、エンドユーザがクライアントとサーバの両方として動作して双方向のエンドツーエンド通信を維持する必要があるため、NATではこれらのUDP接続を確立することが困難です。通常、これらのアプリケーションを動作させるには、NATトラバーサル技術が必要です。

## NATトラバーサルの必要性

インターネット上でのリアルタイムの音声およびビデオ通信は、主流 今日では、VoIPコールをサポートする一般的なインスタントメッセージング(IM)を使用しています。VoIPの最初の採用における大きな障害は、ほとんどのPCまたは他のデバイスがファイアウォールの背後に配置され、プライベートIPアドレスを使用するという事実でした。ネットワーク内の複数のプライベートアドレス(IPアドレスとポート)は、ファイアウォールによって単一のパブリックアドレスにマッピングされます。NAT。ただし、エンドデバイスはパブリックアドレスを認識しないため、VoIP通信でアドバタイズするプライベートアドレスでリモートパーティからの音声トラフィックを受信できません。

片側性 Self-Address Fixing(UNSAF)プロセスは、一部の発信側エンドポイントが、別のエンドポイントに対して既知のアドレス(およびポート)を特定または修正しようとするプロセスです。たとえば、次のことができます uプロトコル交換内のアドレスデータを使用するか、または接続を受信するパブリックアドレスをアドバタイズします。

したがって、検討中のP2P接続はUNSAFプロセスです。P2Pアプリケーションがピアリングセッションを確立して維持する一般的な方法の1つ NAT-friendlyは、NATに対してIPアドレスが公開されているランデブーサーバを使用して、登録とピアディスカバリの目的。

## NAT用のセッショントラバーサルユーティリティ

RFC 5389に従って、STUNはNATを扱うツールを提供します。これは、エンドポイントがプライベートIPアドレスとポートに対応するNATデバイスによって割り当てられたIPアドレスとポートを決定する手段を提供します。また、エンドポイントがNATバインディングを有効に保つ方法も提供します。

### NAT実装のタイプ

UDPのNAT処理は実装によって異なることが確認されています。実装で観察される4つの処理は次のとおりです。

**フルコーン：**フルコーンNATは、同じ内部IPアドレスとポートからのすべての要求が同じ外部IPアドレスとポートにマッピングされるNATです。さらに、どの外部ホストも内部ホストにパケットを送信でき、マッピングされた外部アドレスにパケットを送信します。

**制限付きコーン：**制限付きコーンNATは、同じ内部IPアドレスとポートからのすべての要求が同じ外部IPアドレスとポートにマッピングされるNATです。完全コーンNATとは異なり、外部ホスト ( IPアドレスX ) は、内部ホストが以前にIPアドレスXにパケットを送信した場合にのみ、内部ホストにパケットを送信できます。

**ポート制限付きコーン：**ポート制限付きコーンNATは制限付きコーンNATと似ていますが、ポート番号が制限に含まれます。具体的には、内部ホストが以前にIPアドレスXとポートPにパケットを送信した場合にのみ、外部ホストは内部ホストに送信元IPアドレスXと送信元ポートPを含むパケットを送信できます。

**対称：**対称NATは、同じ内部IPアドレスとポートから特定の宛先IPアドレスとポートへのすべての要求が、同じ外部IPアドレスとポートにマッピングされるNATです。同じホストが同じ送信元アドレスとポートを持つパケットを異なる宛先に送信する場合、異なるマッピングが使用されます。さらに、パケットを受信する外部ホストだけが、UDPパケットを内部ホストに返信できます。

送信元(A、Pa) ( AはIPアドレス、Paは送信元ポート ) がNATデバイスを介して宛先(B、Pb)および(C、Pc)と通信するトポロジを考えてみます。

NAT実装のタイプ	パブリックソース：いつ宛先(B、Pb)	宛先が(C、Pc)	宛先を指定できる(例：(B、Pb) ) Send traffic to (A, Pa)?
円錐全体	(X1、Px1)	(X1、Px1)	Yes
制限付き円錐	(X1,Px1)。	(X1,Px1)。	(A、Pa)が最初にトラフィックをBに送信した場合のみ
ポート制限付き円錐	(X1,Px1)。	(X1,Px1)。	(A、Pa)が最初に(B、Pb)にトラフィックを送信した場合のみ
対称	(X1,Px1)。	(X2、Px2)	(A、Pa)が最初に(B、Pb)にトラフィックを送信した場合のみ

## NATトラバーサルおよび対称NATに関する問題

STUNサーバは、STUNクライアントから送信されたSTUNバインディング要求に応答し、クライアントのパブリックIP/ポートを提供します。このアドレス/ポートは – STUNクライアントがピアツーピア通信で使用する組み合わせ シグナリング。ただしこの時点で エンドホスト は同じプライベートアドレス/ポートを使用します(ここでは、 bound パブリックIP/ポートへ STUN応答で提供される)NATデバイスは同じIPに変換しますが、対称NATの場合は異なるポートに変換します 簡単な私記載を使用します。これにより、UDP通信が切断されます。これは、シグナリングはp以前のポート。

Cisco IOS® ルータ' NAT 簡単な私記載 PATを実行すると、デフォルトでは対称になります。ThereフォアUDP接続の問題が発生する可能性があります IPアドレスを持つ NAT.

ただし、Cisco IOS-XEルータのPAT実行時のNAT実装は対称ではありません。2つの異なる 同じ送信元IPおよびポートを持つ異なる宛先へのストリームでは、送信元は同じ内部グローバルIPおよびポートにNAT変換されます。

## 問題の解決策

この説明から このコマンドを使用すると、この問題は次の手順で解決できます。 エンドポイント非依存 マッピング.

RCFCによる 4787: さらにトラブルシューティングを行うために、 Endpoint-Independent Mapping(EIM)。NATは、同じ内部IPアドレスとポート(X:x)を任意の外部IPアドレスおよびポートに割り当てます。

クライアントから、エンドホストがコマンドnc -p 23456 10.0.0.4 4000およびnc -p 23456 10.0.0.5 50000を2つの異なるターミナルウィンドウで実行した場合、EIMを使用するとNAT変換の結果は次のようになります。

```
Pro Inside global      Inside local           Outside local          Outside global
tcp 10.0.0.1:23456     192.168.0.2:23456    10.0.0.4:40000       10.0.0.4:40000
tcp 10.0.0.1:23456     192.168.0.2:23456    10.0.0.5:50000       10.0.0.5:50000
```

ここでは、同じ送信元アドレスとポートを持つ異なるトラフィックフローが、宛先ポート/アドレスに関係なく、同じアドレス/ポートに変換されることを確認できます。

Cisco IOSルータでは、次のコマンドを使用して、エンドポイント非依存ポート割り当てを有効にできます `ip nat service enable-sym-port`。

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr\\_nat/configuration/15-mt/nat-15-mt-book/iadnat-fpg-port-alloc.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/iadnat-fpg-port-alloc.html)

## 要約

Cisco IOSのNAT実装は、ポートアドレス変換(PAT)を使用する場合にデフォルトで対称になっており、NATトラバーサルにSTUNなどのサーバを必要とするP2P UDPトラフィックを通過する際に問題が発生する可能性があります。これを機能させるには、NATデバイスでEIMを明示的に設定する必要があります。

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。